**8Ш**

**УДК 629.735.05**

***Б.М. Шевчук***
Інститут кібернетики ім. В.М. Глушкова НАН України, м. Київ, Україна
incors@ukr.net

# Захист інформації при передачі пакетів даних в інформаційно-ефективних локально-регіональних радіомережах

У статті обґрунтоване виконання послідовності операцій по захисту інформації в радіомережах з урахуванням досягнення теоретичної стійкості захисту даних абонентами мережі. Зазначено, що основою практично стійкого криптографічного захисту пакетів інформації є використання абонентами мережі шифрів з одноразовим ключем (шифрів Вернама), які від пакета до пакета підлягають зміні. Для захисту інформації про використовуючі сеансові ключі парою абонентів (відправник інформації – отримувач інформації) доцільно використати алгоритми асиметричного криптозахисту. З метою комплексного захисту даних в радіомережах інформація підлягає захисту на інформаційному рівні, на рівні формування сигнальникових конструкцій, на енергетичному рівні.

## Вступ

Широке застосування радіомереж в промисловості, на транспорті в телемедичних системах, в інформаційних системах безпеки руху транспортних засобів, відеомоніторингу та дистанційного моніторингу станів віддалених об’єктів вимагає від розробників інформаційних систем забезпечення конфіденційної та криптостійкої передачі даних в радіоканалі. Як правило, діапазони робочих смуг радіочастот поширених технологій побудови радіомереж (ZigBee, Wi-Fi, WiMax та ін.) відомі багатьом користувачам, тому існує висока ймовірність доступу несанкціонованих абонентів радіомереж до масивів даних, що передаються в пакетах інформації, а також існує висока ймовірність підміни даних та імітації роботи санкціонованих абонентів мережі несанкціонованими користувачами.

На сьогоднішній день в радіомережах для захисту інформації широкого розповсюдження отримали потокові методи шифрування даних [1-4], забезпечується комплекс заходів з аутентифікації і авторизації абонентів мережі та захисту трафіку даних з поєднанням MAC (Media Access Control)-фільтрації з шифруванням WPA (Wi-Fi Protecting Access) та використанням міжмережних екранів. Сучасні інтелектуальні радіомодулі провідних комп’ютерних та мікроелектронних фірм світу для захисту даних в ISM-діапазоні радіочастот (ISM-industrial, scientific, medical: 433 МГц, 868 МГц, 902-928 МГц (для США), 2.4 ГГц) використовують 128-бітне AES-шифрування (AES-Advanced Encryption Standard). В [5] запропонований новий метод захисту даних в комп’ютерних мережах, згідно з яким первинні масиви даних, що підлягають передачі, не шифруються, а замість них передаються ознаки шифрованих даних. При цьому шифрування даних ґрунтується на заміні байтів первинного файла байтами спеціально організованого файла-ключа.

Невирішеними проблемами захисту даних в сенсорних, локальних та локально-регіональних радіомережах є організація передачі пакетів даних між віддаленими абонентами з урахуванням досягнення практичної стійкості криптографічного захисту інформації, яка б максимально відповідала вимогам теоретичної стійкості криптосистеми.

**Метою статті** є розробка та обґрунтування послідовності операцій по захисту інформації в радіомережах з урахуванням досягнення теоретичної стійкості захисту даних абонентами мережі. При цьому виконання елементарних операцій захисту даних поєднується з оптимізацією процесів стиску даних та компактного кодування пакетів інформації, що передаються в каналах зв'язку з шумами. Таким чином, в залежності від продуктивності абонентських процесорних засобів та наявного часу обробки і кодування даних в місцях зародження інформаційних потоків абонентами радіомереж здійснюється ефективне кодування та передача компактних, крипостійких та завадостійких інформаційних пакетів (ІП).

# Обґрунтування доцільності виконання комплексу операцій абонентами мережі для надійного захисту ІП

Основна проблема захисту інформації в комп'ютерних мережах полягає в розповсюдженні абонентських секретних ключів. В ідеальному випадку абонент повинен мати такий секретний ключ (довге число), який не повинен бути відомий іншим абонентам. В той же час процес передачі інформації передбачає, що пара абонентів (відправник інформації – отримувач інформації) повинні володіти інформацією про поточні секретні ключі, які використовуються для шифрування/дешифрування інформаційних кадрів (ІК) пакетів даних. Основою практичної стійкості абонентських секретних ключів (СК) є теоретичні викладки К. Шеннона [6], згідно з якими в системах передачі інформації з цілковитою секретністю необхідно, щоб поточний СК використовувався тільки один раз (тобто після шифрування і передачі бітів поточного ІК даний СК повинен бути замінений на інший), при цьому первинні дані ІК до шифрування $\{X_i\}$, $i = \overline{1,n}$, $n-$ кількість біт ІК, та шифрограма $\{Y_i\}$ повинні бути статистично незалежними для всіх можливих послідовностей бітів масивів $\{X_i\}$ і $\{Y_i\}$. З робіт Шеннона випливає, що в теоретично стійких секретних системах СК за об'ємом не повинні бути меншими, ніж об'єм первинного тексту $\{X_i\}$ та шифрограми $\{Y_i\}$. На практиці прикладом такого шифру є шифр Вернама (шифр з одноразовим ключем), причому захист інформації ґрунтується на виконанні операції додавання за модулем 2 над відповідними бітами двох послідовностей [4], [5]: послідовності бітів первинного масиву даних $X = x_1,...,x_i,...,x_n$ і послідовності випадкових бітів поточного СК $K = k_1,...,k_i,...,k_n$. В результаті виконання операцій додавання за модулем 2 отримуємо криптограму $Y = y_1,...,y_i,...y_n$, для якої справедливий вираз $Y = X \oplus K$, де $y_1 = x_1 \oplus k_1$, …, $y_i = x_i \oplus k_i$, …, $y_n = x_n \oplus k_n$, а $X \oplus 0 = X$, $X \oplus X = 0$. Суттєвою вимогою при виконанні операцій шифрування даних з одноразовим ключем є дотримання вимоги, щоб при виконанні кожної наступної операції шифрування (додавання за модулем 2) використовувався інший, незалежно згенерований СК. Відповідно для $j$-ої операції шифрування парою абонентів, які приймають участь в передачі/прийомі ІП, генерується поточна послідовність випадкових бітів $K_j = k_{1+j},...,k_{i+j},...,k_{n+j}$.

Таким чином базовими операціями захисту масивів даних ІП є використання абонентами мережі операцій генерації довготривалих псевдовипадкових послідовностей (ПВП), гаміювання відповідних масивів даних, формування перевірних кодів (ПерК) ІК пакетів даних та перемішування бітів ІК та бітів ПерК [4], [8]. Величина ступеня захисту інформації $P_z$ пропорційна величинам масивів даних, що підлягають гаміюванню, тобто $P_z \cong max\left[2^m\right]$, де $m-$ мінімально необхідна довжина поточної ПВП, яка використовується для надійного захисту інформації ($m \geq 2048$ біт). В залежності від наявного

часу обробки та кодування даних операцію гаміювання можливо виконувати одноразово, наприклад, після виконання операцій стиску даних без втрат та формування перевірних кодів або кодів, що виправляють помилки. Багаторазове виконання операцій гаміювання даних підвищує ступінь захисту інформації за рахунок спотворення (на основі виконання відповідних операцій гаміювання даних) первинних масивів даних до стиску, в процесі стиску даних без втрат (за рахунок реалізації оперативних алгоритмів стиску-захисту двійкової інформації), після виконання операції перемішування компактних даних ІК з перевірним кодом (кодом, що виправляє помилки) та реалізації кінцевої операції гаміювання. Відповідно без знання абонентських СК несанкціонованим користувачам мережі невідомі масиви даних до стиску і після стиску даних, а також кінцевий масив даних після завадостійкого кодування. Фактично, на інформаційному рівні реалізується ідея К. Шеннона, згідно з якою проблему створення стійкого СК, що не піддається розшифруванню, можна вирішити шляхом побудови такого шифру, розкриття якого було б еквівалентне вирішенню надскладної задачі. Слід зазначити, що елементарні операції захисту інформації на абонентських системах радіомереж є відомими, проте невідомою є комбінація виконання елементарних операцій при формуванні поточних кодів ПВП. Для збереження конфіденційності інформації про абонентські СК доцільно використати алгоритми захисту даних, побудованих на основі асиметричної криптографії з використанням закритих та відкритих абонентських ключів, які (закриті ключі) періодично змінюються центром розповсюдження ключів. З метою реалізації криптостійкої та прихованої передачі інформації в шумах радіоканалу невідомими для сторонніх абонентів мережі повинні бути методи формування сигналів, що підлягають передачі, а також структура цих сигналів [7], [8]. Тому захист даних абонентами радіомережі здійснюється на різних рівнях: на інформаційному рівні, на рівні формування сигнально-кодових конструкцій, що передаються на модулятор радіопередавача, на енергетичному рівні.

## Реалізація оперативного захисту сигналів, зображень, відеоданих та масивів даних на абонентських системах радіомереж

Побудова інформаційно-ефективних радіомереж широкого застосування ґрунтується на реалізації в місцях зародження інформації методів та алгоритмів багатофункціональної обробки і кодування даних (сигналів, відеосигналів, масивів даних) з урахуванням мінімізації вихідних потоків криптостійких та завадостійких ІП. Теоретичною основою для побудови інформаційно-ефективних радіомереж є теорема К. Шеннона про те, що при відповідних способах кодування та модуляції коефіцієнт пропускної здатності каналу зв'язку $\eta = R / C$ може бути дуже близьким до одиниці ($\eta \to 1$), де $R$ – швидкість передачі інформації (біт/с) при двійковому методі кодування, $C$ – пропускна здатність каналу зв'язку (теоретична максимальна швидкість передачі інформації). На практиці коефіцієнт $\eta \to 1$ при постійній підтримці швидкості передачі інформації $R \to R_{max}$ в умовах зміни співвідношення сигнал/шум в каналі зв'язку у великих межах. Відповідно основою побудови інформаційно-ефективних радіомереж є формування абонентами мережі компактних (з мінімальною тривалістю), криптостійких та завадостійких пакетів даних [9].

При кодуванні сигналів, які характеризуються мінімальними і максимальними значеннями амплітудних і частотних параметрів, відповідно $X_{min}$ і $X_{max}$ та $f_{min}$ і $f_{max}$, доцільно виявляти та компактно кодувати найбільш інформативні (суттєві) відліки, до яких відносяться екстремуми та точки перегину огинаючої (точки зміни опуклості

кривої). З метою компактного кодування суттєвих відліків сигналу опосередковано визначається вхідне співвідношення сигнал/шум в околиці суттєвих відліків $[c/ш]_{вх}$ та середня крутизна сигналу [4]. Отримані додаткові параметри відліків сигналів дозволяють вибрати (закодувати) оптимальну частоту дискретизації сигналу $f_д$ та кількість біт $q$ для кодування відліків сигналів. Компактне кодування суттєвих відліків здійснюється з контрольованими втратами, тобто на чистих від шумів ділянках суттєві відліки кодуються більш точно в порівнянні з відліками на зашумлених ділянках.

При кодуванні відеоданих необхідно враховувати особливості вихідних потоків сучасних відеосенсорів, які суттєво залежать від формату відеокадру, прийнятої схеми кольорового відеокодування, топології побудови світлофільтрів відеосенсора та формату вихідних даних. У випадку використання відеосенсорів з поширеною $RGBG$-топологією розміщення піксельних світлофільтрів матриці зображення розміром $M \times N$ ($M$ – кількість пікселів у рядку, $N$ – кількість пікселів у стовпчику (кількість рядків)), вихідні відеодані передаються процесорним пристроям від кадру до кадру. При цьому коди відповідних пікселів рядок за рядком по паралельній шині передаються на входи процесора. З метою якісного відображення відеоданих для кожного пікселя необхідно визначати три складові *R*-, *G*-, *B*-відліки, де $R$, $G$ і *B*-коди червоного, зеленого і синього відліків відповідно. Таким чином формуються *R*-, *G*-, і *B*-сигнали, компактне кодування яких нічим не відрізняється від кодування аналогового сигналу (пошук суттєвих відліків та компактне кодування службових та інформативних бітів). Після аналізу та визначення амплітудно-часових характеристик суттєвих відліків на інтервалі вибірки відповідного сигналу, наприклад, поточного рядка або групи рядків матриці $M \times N$, здійснюється компактне кодування даних з урахуванням наявності загальної службової інформації, службової інформації і компактних даних суттєвих і несуттєвих відліків відповідних рядків чи групи рядків поточного кадру. Для досягнення заданого коефіцієнту стиску відеоданих при збереженні максимальної точності параметрів суттєвих відліків здійснюється рейтинговий або пороговий відсів найбільш інформативних суттєвих відліків відеосигналів. Подальшим резервом стиску відеоданих є компактне кодування змін між групою сусідніх відеокадрів.

Отримані компактні масиви даних з контрольованими втратами відліків сигналів (відеосигналів) підлягають подальшому стиску на основі оперативного та адаптивного способу стиску бітових масивів даних. В процесі стиску масивів без втрат ефективно реалізується захист інформації з урахуванням відповідних кодів згенерованої ПВП. Як правило, будь-який масив двійкових даних характеризується нерівномірним розподілом *n*-бітових послідовностей, де $n$ = 3, 4, 5, 6, ... . Здійснивши кодування первинних масивів даних з використанням відповідних шифрів з багаторазовою підстановкою, можливо суттєво спотворити вміст масивів даних. При цьому істинний об'єм вихідного зашифрованого масиву даних буде меншим за первинний масив даних. Тому таку комплексну операцію можна назвати операцією «стиску-захисту» даних. За рахунок гамiювання даних можливо змінювати характеристики розподілу *n*-бітових послідовностей, а поєднання операцій гамiювання та багаторазової підстановки двійкових послідовностей дозволяє надійно захистити масиви даних, що підлягають накопиченню та передачі по каналам зв'язку. Для формування довготривалих ПВП доцільно використати генератори М-послідовностей з надвеликими утворюючими поліномами, наприклад, $X^{163} + X^7 + X^6 + X^3 + 1$ [10], а також $X^{41} + X^{20} + 1$, $X^{41} + X^3 + 1$ [11]. З метою генерації криптостійких ПВП кожний абонент використовує таблицю кодових ключів генерації бітів ПВП. На початку кожного циклу генерації довготривалих ПВП, для підвищення її криптостійкості, випадковим чином змінюють послідовність слідування табличних номерів кодових ключів генерації елементарних ПВП. Використовуючи циклічно задану кількість бітів абонентського СК (поточного СК) гамiюємо біти кож-

ного табличного номера кодового ключа з поточними бітами СК. Таким чином утворюється додаткова таблиця кодових ключів з псевдовипадковим розміщенням номерів кодових ключів. Із додаткової таблиці беремо два сусідніх кодових ключа, генеруємо їх, утворивши поточний фрагмент елементарної ПВП, яка у свою чергу гаміюється з бітами ПВП, згенерованої на основі використання одного із надвеликих кодових ключів. Для уникнення довготривалих однотипних бітових послідовностей у вихідному потоці ПВП (довгих послідовностей нульових чи одиничних бітів) після прорахунку допустимої величини однотипних бітів (цю величину можна змінювати в заданих межах випадковим чином) доцільно інвертувати наступний однотипний біт.

Таким чином кожний абонент мережі володіє закритим секретним ключем, який невідомий іншим абонентам, а також володіє базою даних кодових ключів для генерації ПВП. При необхідності передачі пакетів даних *j*-му абоненту мережі *i*-й абонент направляє *j*-му абоненту коротке повідомлення і після отримання підтвердження від *j*-го абонента, направляє останньому сеансовий ключ (випадкове число), зашифрований засобами асиметричної криптографії. Після цього здійснюється передача ІП, зашифрованих сеансовим ключем. Альтернативним способом вирішення проблеми обміну ключами між абонентами радіомережі без використання засобів асиметричної криптографії є наступний: центр розподілу ключів генерує сеансовий ключ для передачі поточних пакетів, а далі доставляє сеансовий ключ, зашифрований за допомогою секретних ключів кожного з двох абонентів. Після дешифрування повідомлення про сеансовий ключ абоненти використовують його при передачі ІП до наступної зміни сеансового ключа.

## Висновки

При передачі пакетів інформації в радіомережах з урахуванням досягнення практичної стійкості криптографічного захисту інформації, яка б максимально відповідала вимогам теоретичної стійкості криптосистеми, необхідно кожний інформаційний кадр поточного пакета шифрувати своїм секретним шифром. Відповідно шифри від пакета до пакета повинні бути різними, при цьому первинні дані поточного інформаційного кадру та його шифрограма повинні бути статистично незалежними масивами даних. Основою практично стійкого криптографічного захисту пакетів інформації є використання абонентами мережі шифрів з одноразовим ключем (шифрів Вернама). Базовими операціями захисту пакетів є генерація абонентами довготривалих псевдовипадкових послідовностей, гаміювання відповідних масивів даних, формування перевірних кодів або кодів, що виправляють помилки, та перемішування бітів інформаційного кадру та перевірних бітів. Для збереження конфіденційності інформації про абонентські секретні ключі доцільно використати алгоритми захисту даних (для передачі сеансових ключів), побудованих на основі асиметричної криптографії. З метою реалізації криптостійкої та прихованої передачі інформації в шумах радіоканалу невідомими для сторонніх абонентів повинні бути методи формування сигналів, що підлягають передачі, а також структура цих сигналів. Відповідно захист даних абонентами радіомережі повинен бути на різних рівнях: на інформаційному, на рівні формування сигнально-кодових конструкцій, на енергетичному рівні. Для побудови інформаційно-ефективних радіомереж шляхом мінімізації абонентами вихідних потоків криптостійких та завадостійких пакетів доцільно на кожній абонентській системі мережі реалізувати стиск-захист масивів даних на основі оперативного та адаптивного способу стиску бітових послідовностей. Для цього доцільно поєднати операції гаміювання та багаторазової підстановки двійкових послідовностей. Для формування довготривалих криптостійких псевдовипадкових послідовностей доцільно абонентами мережі використовувати базу даних кодових ключів для генерації ПВП, серед яких є ключі генерато-

рів, наприклад, М-послідовностей з надвеликими утворюючими поліномами. При цьому при формуванні абонентами результуючої ПВП забезпечуються умови псевдовипадкового використання відповідних кодових ключів. Альтернативний спосіб вирішення проблем шифрування/дешифрування даних ІП (без використання засобів асиметричної криптографії) полягає в передачі та використанні абонентами сеансового ключа, зашифрованого відповідними абонентськими ключами.

# Література

1. Столлингс В. Основы защиты сетей : приложения и стандарты / Столлингс В. – М. : Издательский дом «Вильямс», 2002. – 429 с.
2. Шахнович И.В. Современные технологии беспроводной связи, 2-е изд. / Шахнович И.В. – М. : Техносфера, 2006. – 288 с.
3. Зубов А. Совершенные шифры / Зубов А. – М. : Гелиос АРВ, 2003. – 160 с.
4. Шевчук Б.М. Ефективні методи фільтрації-стиску та захисту інформації в комп'ютерних мережах тривалого моніторингу станів об'єктів / Б.М. Шевчук, В.К. Задірака, С.В. Фраєр // Штучний інтелект. – 2006. – № 3. – С. 804-815.
5. Алишов Н.И. Косвенная стеганография как новый способ защиты компьютерных данных / Н.И. Алишов, В.А. Марченко, С.Г. Оруджева // Комп'ютерні засоби, мережі та системи. – 2009. – № 8. – С. 105-112.
6. Шеннон К. Теория связи в секретных системах / К. Шеннон // Работы по теории информации и кибернетике. – М. : Изд. иностр. лит., 1963. – С. 333-369.
7. Шевчук Б.М. Защита информации в компьютерных мониторинговых сетях на основе маскирования сжатых данных и передачи псевдослучайных шумоподобных пакетов информации / Б.М. Шевчук, С.В. Фраєр // Компьютерная математика. – 2006. – № 1. – С. 80-87.
8. Урядников Ю.Ф. Сверхширокополосная связь. Теория и применение / Ю.Ф. Урядников, С.С. Аджемов. – М. : СОЛОН-Пресс, 2005. – 368 с.
9. Шевчук Б.М. Моделі та методи обробки, кодування і передачі інформації для побудови інформаційно-ефективних комп'ютерних мереж / Б.М. Шевчук // Комп'ютерні засоби, мережі та системи. – 2009. – № 8. – С. 81-89.
10. ДСТУ 4145 – 2002. Державний стандарт України. Інформаційні технології : Криптографічний захист інформації. Цифровой підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.
11. Новые алгоритмы формирования и обработки сигналов в системах подвижной связи / А.М. Шлома, М.Г. Бакулин, В.Б. Крейнделин, А.П. Шумов ; под ред. А.М. Шломы. – М. : Горячая линия-Телеком, 2008. – 344 с.

***Б.М. Шевчук***

**Защита информации при передаче пакетов данных в информационно-эффективных локально-региональных радиосетях**

В статье обосновано выполнение последовательности операций по защите информации в радиосетях с учётом достижения теоретической стойкости защиты данных абонентами сети. Отмечено, что основой практически стойкой криптографической защиты пакетов информации является использование абонентами сети шифров с одноразовым ключом (шифров Вернама). Для защиты информации об используемых сеансовых ключах парой абонентов (отправитель информации – получатель информации) целесообразно использовать алгоритмы защиты данных, построенные на основе асимметричной крипторгафии. С целью обеспечения комплексной защиты данных в радиосетях информация защищается на разных уровнях: на информационном уровне, на уровне формирования сигнально-кодовых конструкций, на энергетическом уровне.

***B.M. Shevchuk***

**Protection in the Transmission of Information Packets in the Effective Local-Regional Radio Networks**

In the article the performance of sequences of operations for the protection of information in radio networks with regard to achieve the theoretical strength of data protection network subscribers. It is noted that the basis of virtually resistant cryptographic protection of information packets is to use a subscriber network is encrypted with a one-time key (Vernam's cipher). To protect the information on the use of session keys, a pair of users (the sender information, recipient information) should be used for data protection algorithms built on the basis of asymmetric cryptography. In order to ensure comprehensive data protection in Radio the information is protected at various levels: at the information level, the level of formation of signal-code structures, the energy level.

*Стаття надійшла до редакції 28.05.2010.*